POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Fecha	Responsable
14/07/2025	**Elaborado por:** Ing. Uberto Gonzáles Bendezú Sub Gerente de Tecnologías de la Información
14/07/2025	**Revisado por:** Ing. Fredy Sánchez Quispe Subgerente de Planeamiento y Control de Gestión
	Homologado por: Ing. Carlos Menéndez Deza Gerente General
	Aprobado por: Directorio

Control de Cambios		
Versión	**Descripción del Cambio**	**Fecha**
01	Resolución de GG N.° 147-2016	30/12/2016
02	Sesión de Directorio N.° 672	17/11/2020
03	Sesión de Directorio N.° 744	25/07/2023
04	Sesión de Directorio N.° 796	24/07/2025

1. Objetivo General

Establecer políticas específicas de seguridad de la información con el propósito de proteger y gestionar los activos de información, controlar los riesgos asociados y mantener un esquema de seguridad fundamentado en los principios de confidencialidad, disponibilidad e integridad. Todo esto, en coherencia con la Política y los Objetivos de Seguridad de la Información definidos en el Sistema de Gestión Integrado de EGEMSA[1].

2. Alcance

Las presentes Políticas Específicas son de aplicación obligatoria para todas las áreas y los/as usuarios/as comprendidos dentro del alcance del Sistema de Gestión de Seguridad de la Información de la Empresa de Generación Eléctrica Machupicchu, en lo que respecta al cumplimiento de los controles establecidos en la Declaración de Aplicabilidad[2].

3. Base Legal

- Decreto Legislativo N.º 1693, que ordenó, sistematizó y optimizó la eficiencia de la Actividad Empresarial del Estado y fortaleció la estructura y gestión del FONAFE[3].

- Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y modificatorias[4].

- Decreto Supremo N.° 029-2021-PCM, Reglamento del Decreto Legislativo Nro. 1412, modificado mediante Decreto Supremo Nro. 075-2023-PCM[5].

- Decreto Supremo N.° 050-2018-PCM, que aprueba la definición de Seguridad Digital de Ámbito Nacional[6].

- Resolución Ministerial N.° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnica de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática y modificatorias[7].

- Resolución Ministerial N.° 087-2019-PCM, Resolución Ministerial que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital[8].

- Directiva Corporativa de Gestión Empresarial, aprobada mediante Acuerdo de Directorio N.° 003-2018/006-FONAFE y modificatorias[9].

- Código de Buen Gobierno Corporativo para las Empresas bajo el ámbito de FONAFE, aprobado mediante Acuerdo de Directorio N.° 002-2013/003-FONAFE[10].

- Lineamiento Corporativo: “Lineamiento de Gestión Integral de Riesgos para las Empresas bajo el ámbito de FONAFE”, aprobado mediante Resolución de Dirección Ejecutiva N.° 030-2018/DE-FONAFE[11].

- Lineamiento Corporativo: “Lineamiento del Sistema de Gestión de Seguridad de

la Información", aprobado mediante Resolución de Dirección Ejecutiva N.° 029-2020/DE-FONAFE[12].

- Vinculadas a la implementación de la Norma Técnica Peruana "NTP ISO/IEC Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información 27001:2022[13].

4. Términos y/o definiciones

- **Autenticación**: Proceso de confirmación o verificación de alguien que es o que dice ser[14].

- **Base de datos**: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso[15].

- **Activos de información**: Conocimientos o datos que tienen valor para la Institución, viene a ser lo que una entidad valora y por lo tanto debe proteger, estos pueden ser: los datos creados o utilizados por un proceso, recursos o documentación (digital, papel u otro medio)[16].

- **Cadena de custodia:** Procedimiento controlado que implica la extracción, transporte y entrega de la información[17].

- **Código malicioso:** Programas informáticos que tienen por objetivo ingresar al sistema de información sin que se detecte su presencia vulnerando la información de EGEMSA, sus vías de diseminación son: el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles[18].

- **Contratista:** Es la parte interesada que tiene una relación contractual con la Empresa, de conformidad con las disposiciones de la Ley N.° 32069, Ley General de Contrataciones Públicas y su Reglamento, aprobado mediante Decreto Supremo N.° 009-2025-EF[19].

- **Criptografía:** Estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican[20].

- **Custodio:** Persona responsable de administrar controles autorizados por los propietarios de los activos de información, protegiendo los activos asignados para su custodia[21].

- **Documentos de gestión:** procedimientos, instructivos, formatos, cartillas u otros lineamientos asociados a la evidencia del sistema de gestión y tienen injerencia dentro del alcance SGSI[22].

- **Equipamiento perimetral:** Integra elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos de la red de EGEMSA[23].

- **Gestión de incidentes**: Acción que se lleva a cabo para conseguir o resolver un incidente ante un impedimento de la operación o una violación a las Políticas de Seguridad de la Información[24].

- **No repudio:** Imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil[25].

- **Practicante preprofesional**: Estudiante de un Centro de Formación Profesional[26].

- **Privilegios:** Ventaja exclusiva o especial que goza por concesión de un superior[27].

- **Procesamiento de información:** Técnicas eléctricas, electrónicas o mecánicas usadas para manipular datos para el empleo humano o de máquinas[28].

- **Propietario de activo de información:** Servidor/a civil que en atención a sus funciones se le han asignado la responsabilidad de gestionar un activo de información. El término "propietario" no significa que la persona tenga en realidad derechos de propiedad sobre el activo[29].

- **Recursos informáticos:** Componentes de hardware y software que son necesarios para el buen funcionamiento y la optimización del trabajo con computadoras[30].

- **Recuperación de información:** Conjunto de actividades orientadas a facilitar la localización y restauración de determinados datos y sus interrelaciones[31].

- **Respaldo de información:** Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida[32].

- **Colaborador:** Personal de EGEMSA que se encuentra contratado/a bajo el Texto Único Ordenado del Decreto Legislativo N.° 728, Ley de Productividad y Competitividad Laboral, aprobado mediante Decreto Supremo N.° 003-97-TR[33].

- **Sistema de Gestión:** Gestión de servicios que se ofrecen, y que incluye planear, controlar y mejorar[34].

- **Tercero/a:** Persona, natural o jurídica, inscrita en el Registro de Terceros del EGEMSA[35].

- **Trazabilidad**: Seguimiento de los documentos desde su creación hasta su disposición final[36].

- **Usuario/a:** Colaborador/a, contratista, tercero/a seleccionado/a practicante, practicante profesional y serumnista, que tenga vínculo laboral o contractual con EGEMSA; o, se encuentre en alguna modalidad formativa, según corresponda; y, use habitualmente el hardware y software brindados por EGEMSA[37].

5. Políticas Especificas

En el marco del compromiso con la mejora continua del Sistema de Gestión de

Seguridad de la Información, y en concordancia con la Norma Técnica Peruana de Sistemas de Gestión de Seguridad de la Información, aprobada mediante Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/DNB-INDECOPI, así como con la Política Integrada del Sistema de Gestión Integrado de EGEMSA[38].

5.1. Dispositivos terminales de usuario y Trabajo Remoto

Objetivo: Asegurar la seguridad del uso de los dispositivos terminales de usuario y trabajo a distancia[39].

EGEMSA, en el marco de la Seguridad de la Información, establecen los siguientes compromisos[40]:

a) Establecer los controles y medidas de seguridad de apoyo adoptados para la gestión de los riesgos asociados a la protección de la información en el uso de dispositivos móviles de propiedad de EGEMSA. Dichas disposiciones deberán ser formalizadas mediante los correspondientes documentos de gestión interna y deberán contemplar, entre otros mecanismos, los referidos a[41]:

   - El registro de los dispositivos móviles[42].
   - La restricción de instalación de software[43].
   - Sistema de protección contra software malicioso[44].
   - Control de acceso a las aplicaciones[45].

b) Establecer los controles y medidas de seguridad para proteger la información que se acceda, procese, almacene, transfiera o cualquiera que sea su tratamiento; en la modalidad del trabajo a distancia, a través de los respectivos documentos de gestión interna, que contemplen, entre otros mecanismos, referidos a[46]:

   - Acciones vinculadas al fortalecimiento de los conocimientos y sensibilización del uso de la información y equipos a los/as usuarios[47].
   - Acciones vinculadas a[48]:

     i. La seguridad de la información con los/las servidores/as civiles, practicantes y profesionales que realizan sus funciones y actividades a través de la modalidad de trabajo a distancia; y,[49]
     ii. Los equipos de propiedad de EGEMSA[50].
   - Mantenimiento y sostenibilidad del acceso remoto a los sistemas internos de EGEMSA[51].

c) Custodiar y gestionar licencias de software en las estaciones de trabajo de los/as servidores/as civiles[52].

d) Establecer controles cuando se acceda a la información a través de dispositivos que no pertenezcan a EGEMSA, referidos a[53]:

   - No dejar desatendidos los equipos cuando se acceda a información[54].
   - Tomar precaución sobre el acceso a los dispositivos por usuarios no autorizados[55].
   - Mantener los métodos de autenticación y control de accesos según las

políticas de control de accesos[56].

5.2. Uso aceptable de la información y otros activos asociados

Objetivo: Identificar los activos de EGEMSA y definir reglas y responsabilidades de protección apropiadas[57].

EGEMSA, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[58]:

a) Identificar, elaborar y mantener actualizado el inventario de activos de información e instalaciones de procesamiento de información pertenecientes a los procesos del alcance del Sistema de Gestión de Seguridad de la Información, a través de las Matrices de Análisis y Evaluación de Riesgos SGSI[59].

b) Asignar a un/a propietario/a del activo de la información y demás activos asociados a los recursos, para el tratamiento de la información que forman parte del inventario[60].

c) Establecer reglas a los/as usuarios/as para el uso adecuado de los activos relacionados con el tratamiento de la información, referidas a[61]:

- Asegurar la información evitando su exposición o divulgación; de acuerdo con su clasificación[62].
- Limitar el uso de equipos informáticos de pertenencia personal para desempeñar sus funciones, servicios o actividades[63].
- Usar los activos de información únicamente para el desarrollo de sus funciones o servicios, de acuerdo al marco normativo vigente y las políticas de seguridad de la información; con el objeto de evitar daños operativos, a la imagen o a otros intereses de EGEMSA[64].
- Restringir los servicios de la red que puedan dañar, deshabilitar, sobrecargar o deteriorar algún otro equipo[65].
- Proteger la identidad de usuario/a con el fin de evitar la suplantación sobre el origen de las comunicaciones u otro contenido; así como cualquier actividad que intente la recopilación de información de cualquier equipo o sistema con propósitos no establecidos ni acordados previamente[66].
- Devolver todos los activos de EGEMSA que le fueron brindados para el desarrollo de sus funciones, servicios o actividades, al término del vínculo laboral, contractual o modalidad formativa[67].
- Informar de cualquier supuesto incidente, debilidad, o evento de seguridad, de tal manera de ejecutar las actividades para la investigación y eliminación de éstos[68].

5.3. Control de acceso

5.3.1. Requisitos de EGEMSA para el control de acceso

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información[69].

EGEMSA, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[70]:

a) Establecer los controles de acceso basados en los requisitos y/o necesidades de la EGEMSA y de la seguridad de la información, a través de documentación de privilegios de acceso[71].

b) Establecer disposiciones referidas al control de acceso físico a EGEMSA y sus ambientes, mediante los respectivos documentos de gestión interna[72].

c) Brindar el acceso a los/as usuarios/as solamente a la red y servicios que hayan sido específicamente autorizados a usar. Para lo cual, se establecen y/o actualizan los respectivos documentos de gestión interna, que regulan[73]:

- Los requerimientos de acceso y autorización a plataformas (sistemas de información), aplicaciones (cliente servidor), servicios de instalaciones (software de diseño, ofimática, entre otros), base de datos o cualquier otro recurso informático de EGEMSA[74].
- Los tipos de perfiles (usuario general/usuario con privilegios especiales) para el acceso a plataformas, aplicaciones, servicios y base de datos[75].

5.3.2. Gestión de acceso de el/la usuario/a

Objetivo: Asegurar el acceso de los/as usuarios/as autorizados/as y prevenir el acceso no autorizado a los sistemas y servicios[76].

EGEMSA en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[77]:

a) Establecer mediante documentos de gestión interna las acciones referidas a[78]:

- Autorizar y solicitar el acceso a los sistemas de información y servicios informáticos para los/as usuarios/as[79].
- Solicitar a la Subgerencia de Tecnologías de la Información la baja de usuarios/as al finalizar su vínculo laboral o contractual o modalidad formativa[80].
- La asignación o revocación de los derechos de acceso según los tipos de usuarios (usuario general/ usuario con privilegios especiales) a los sistemas, servicios informáticos y base de datos en función a sus actividades[81].
- Restringir y controlar la asignación y uso de derechos de acceso privilegiado a los/as usuarios[82].

b) Establecer los controles adoptados para la asignación de información de autentificación secreta, a través de los respectivos documentos de gestión interna, los cuales consideran que[83]:

- Los/as usuarios/as son responsables de la actividad asociada a su usuario de red y a las funciones, servicios o actividades asignadas[84].
- Las contraseñas requieren cierto nivel de complejidad mínimo y no pueden estar asociadas a datos personales que permitan su deducción, como, por ejemplo: nombres propios, nombre de usuario de red, números de documento, dirección, teléfono, entre otros[85].
- Los criterios para establecer una contraseña segura son[86]:
    - Longitud mínima de ocho (8) caracteres[87].

- No usar contraseñas anteriores[88].
- Estar formada por al menos tres (3) características de las siguientes[89]:
  - Caracteres alfabéticos en mayúsculas y/o en minúsculas[90];
  - Caracteres numéricos[91];
  - Caracteres especiales o extendidos[92];
- La validez de las contraseñas no podrá superar los tres (3) meses[93].
- Se realiza el bloqueo de la cuenta luego de cinco (5) reiterados intentos fallidos de inicio de sesión[94].

c) Revisar semestralmente los derechos de acceso de usuario (red, aplicaciones); así como los usuarios con privilegios, a fin de mantener un control eficaz del acceso a los datos y servicios de información[95].

d) Revisar las alertas de expiración de contraseñas de usuario finales y usuarios de aplicación de base de datos, que son notificadas por correo electrónico de forma automatizada, a fin de mantener un control eficaz del acceso a los datos[96].

e) Remover o adaptar los derechos de acceso a la información e instalaciones de procesamiento de información (incluyendo acceso físico y lógico, llaves, mecanismos de identificación y retiro de cualquier documentación) a los/las usuarios/as de acuerdo con el término de su vínculo laboral o contractual o modalidad formativa[97].

5.3.3. Control de acceso a los sistemas y aplicaciones

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones[98].

EGEMSA, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[99]:

a) Establecer los documentos de gestión interna para el acceso a la información y a las funciones del sistema[100].

b) Asegurar que los sistemas de información incluyan mecanismos automáticos de gestión de acceso (tales como: bloqueo después de un tiempo de inactividad, obligación de cambio de contraseña, entre otros)[101].

c) Restringir el acceso al código fuente de los programas que EGEMSA custodia y/o administra[102].

5.4. Uso de la Criptografía

Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información[103].

EGEMSA, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[104]:

a) Usar controles criptográficos incluyendo técnicas de enmascaramiento para la

protección de la información, con el fin de asegurar una adecuada protección de su confidencialidad e integridad, en los siguientes casos[105]:

- Para la protección de las claves de acceso a los sistemas, datos y servicios[106].
- Para la transmisión de información clasificada como confidencial[107].
- Para el resguardo de información[108].

b) Usar, proteger, establecer y verificar el tiempo de vida de las claves criptográficas, a través de los respectivos documentos de gestión interna[109].

5.5. Protección contra la seguridad física y ambiental

Objetivo: Prevenir el acceso no autorizado, la pérdida, daño o robo de activos e interrupción de las operaciones de la EGEMSA[110].

EGEMSA, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[111]:

a) Verificar que los equipos informáticos no se encuentren expuestos a amenazas y/o peligros ambientales; de acuerdo con los documentos de gestión interna que se implementen y que las áreas cumplan dicho fin[112].

b) Prohibir la apertura y traslado de los equipos informáticos por parte de los usuarios; salvo, previa autorización de la Subgerencia de Tecnologías de la Información, en caso corresponda[113].

c) Proteger los equipos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro[114].

d) Asegurar que los cables que transportan datos se encuentren debidamente protegidos contra la interceptación, interferencia o posibles daños[115].

e) Efectuar el mantenimiento de los equipos informáticos de EGEMSA[116].

f) Aplicar controles de seguridad de la información en los equipos informáticos de propiedad de EGEMSA a emplearse en la modalidad de trabajo a distancia[117].

g) Asegurar que la información clasificada como no pública sea borrada de manera irreversible; así como también en el caso que contengan software propietario, cuando se encuentre en medios de almacenamiento que serán reutilizados, reemplazados o dados de baja[118].

h) Establecer la protección apropiada para los equipos desatendidos, lo cual es de conocimiento de los/las usuarios[119].

i) Para la documentación y equipos, se cumple con lo siguiente[120]:

Pantalla Limpia:

- El/la usuario/a al ausentarse de su puesto donde desarrolla funciones, servicios o actividades debe bloquear la sesión de los equipos de cómputo mediante las teclas CTRL + ATL + SUPR (opción bloquear) o tecla Windows

+ L, para proteger el acceso a las aplicaciones y servicios de EGEMSA de personas no autorizadas[121].

- La Subgerencia de Tecnologías de Información implementa el bloqueo automático de la sesión de usuario mediante el directorio activo al transcurrir cinco (5) minutos de inactividad en el equipo de cómputo[122].

- La Subgerencia de Tecnologías de Información de manera coordinada con la Oficina de Relaciones Institucionales determinan y configuran el fondo de pantalla institucional de los equipos de cómputo de EGEMSA[123].

- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los funcionarios o contratistas ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso[124].

Escritorio Limpio:

- Los puestos donde el/la usuario/a desarrolla sus funciones, servicios o actividades deben permanecer limpios y ordenados[125].

- Cuando se imprima o digitalice documentos con información no pública, estos deben retirarse inmediatamente de dichos dispositivos[126].

- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos y estar protegidos de su uso no autorizado[127].

- Los documentos que elaboren los/as usuarios/as, en el ejercicio de sus funciones y actividades o en el cumplimiento de sus obligaciones contractuales, según sea el caso, deben guardarse en la carpeta de almacenamiento en red o almacenamiento en la nube dispuesta por EGEMSA[128].

- Los gabinetes, cajones y archivadores que contienen documentos y/o medios extraíbles con información, deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral, actividades o servicios[129].

- El/la usuario/a debe apagar los equipos informáticos que use al culminar su jornada laboral, actividades o servicios en el día, de ser aplicable y bajo la modalidad de trabajo[130].

- Reportar a la mesa de ayuda “soportetic1@egemsa.com.pe” cualquier solicitud de soporte con referencia al uso de activos[131].

5.6. Transferencia de información

Objetivo: Mantener la seguridad de la información intercambiada dentro de EGEMSA y con cualquier otra entidad[132].

EGEMSA, en el marco de su compromiso con la Seguridad de la Información, propone e implementa controles de seguridad de la información para proteger el intercambio de información por medio del uso de cualquier tipo de recurso de comunicación, en función a su clasificación[133].

Asimismo, el/la jefe, director/a, subdirector/a o coordinador/a del área usuaria tienen el compromiso de[134]:

a) Asegurar la implementación de controles de seguridad de la información para la transferencia de la información según su clasificación[135].

b) Establecer acuerdos y/o cláusulas de confidencialidad y no divulgación previa a la transferencia de información que no sea de carácter público ya sea dentro de EGEMSA o contra una entidad externa[136].

c) Intercambiar información (incluyendo la trazabilidad, no repudio, cadena de custodia, control de acceso) entre las diferentes áreas de EGEMSA y fuera de este, en función de los roles, servicios y actividades de cada servidor/a civil, contratista, tercero/a seleccionado/a, practicante pre-profesional y profesional[137].

d) Asegurar el correcto direccionamiento y transporte de la mensajería electrónica[138].

e) Incorporar al acuerdo de transferencia de información, de ser aplicable, lo siguiente[139]:

- Responsabilidades en caso de incidentes de seguridad de la información tales como la pérdida de los datos[140].
- Cualquier control especial necesario para proteger elementos sensibles como criptografía[141].
- Mantener una cadena de custodia para la información durante el tránsito[142].
- Niveles aceptables de control de acceso[143].

f) Considerar para el acceso de terceros/as seleccionados/as y contratistas la información reservada o confidencial, los siguientes requisitos[144]:

- Definición de la información que se protegerá[145].
- Duración esperada del acuerdo, en caso sea necesario mantener la confidencialidad de manera indefinida[146].
- Acciones necesarias al terminar un acuerdo[147].
- Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada[148].
- Propiedad de la información, la propiedad intelectual y cómo esta se relaciona con la protección de información confidencial[149].
- El uso permitido de la información y los derechos del firmante para utilizar la información[150].
- El proceso para la notificación y reporte de la divulgación no autorizada o fuga de información confidencial[151].
- Términos para la devolución o destrucción de la información al término del acuerdo[152].
- Medidas esperadas que se tomarán en caso de un incumplimiento del acuerdo[153].

g) Contar con la autorización del/ la responsable de los activos de información para el retiro y/o desplazamiento de estos de los ambientes de procesamiento, almacenamiento y comunicación de información, utilizando los medios de transporte autorizados por EGEMSA[154].

h) No comprometer a EGEMSA en casos de difamación, acoso, suplantación, reenvío de mensajes en cadena, entre otros[155].

El/la propietario/a de la información analiza, evalúa y define el alcance de la transferencia de la información que realizarán con otras partes interesadas para darle los controles de seguridad, al transferir información que no sea de carácter público. Para ello, EGEMSA tiene el compromiso de[156]:

a) Asegurar que la información cuya clasificación no es pública, solo sea compartida entre los/as usuarios/as autorizados/as por el/la propietario/a de la información y contando con los controles, concordancia con su clasificación[157].

b) Evitar que los documentos con información que no sea de carácter público sean expuestos a personas no autorizadas mientras permanezca bajo su custodia (incluye el proceso de impresión)[158].

c) Acatar las disposiciones del buen uso del correo institucional, internet y servicio de telefonía emitidas por EGEMSA[159].

5.7. Ciclo de vida de Desarrollo seguro

Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información[160].

En ese sentido, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[161]:

a) Establecer disposiciones para el desarrollo de software y sistemas seguros para EGEMSA[162].

b) Establecer y aplicar procedimientos de control de cambio a los sistemas de información dentro del ciclo de vida del desarrollo[163].

c) Garantizar que el ambiente de desarrollo debe de mantenerse seguro y siempre separado del ambiente de pruebas y de producción, debiendo existir controles de acceso adecuados para cada uno de ellos[164].

d) Evitar la alteración de los sistemas de información, que no sean aprobados por los/as propietarios/as de los activos de información[165].

e) Garantizar los cambios en las plataformas operativas, a través de la implementación de controles, pruebas y verificación, antes de su despliegue en el ambiente de producción, incluyendo respaldos, recursos, criterios de aceptación del cambio y un plan de rollback (retornar a una versión anterior)[166].

f) Proteger el acceso a la información de producción que contenga datos sensibles de los/as usuarios/as que desarrollen funciones y/o actividades de programación en EGEMSA[167].

g) Los sistemas desarrollados o modificados por terceras partes deben cumplir con lo establecido en la presente Política, incluyendo los criterios de seguridad[168].

h) Establecer con los/as usuarios/as cláusulas previas y/o acuerdos que

resguarden la propiedad intelectual y aseguren los niveles de confidencialidad de la información manejada en los proyectos[169].

i) Supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente[170].

j) Establecer gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, asociada a proponer las medidas de mitigación al riesgo definido. Al menos una vez al año se debe realizar un escaneo de las aplicaciones, servicios y sistemas operativos en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas[171].

k) Efectuar validaciones y evaluaciones de seguridad y funcionalidad durante las etapas del ciclo de vida del proyecto[172].

l) Incluir en los programas críticos, la generación de registros de auditoría, considerando como mínimo la identidad de el/la usuario/a que lee o escribe, la fecha y hora, y el IP de origen. Estos registros deben ser protegidos contra la manipulación no autorizada[173].

m) Establecer, documentar y aplicar principios de seguridad en ingeniería de sistemas para la implementación de los sistemas de información[174].

n) Inscribir y/o registrar en INDECOPI, a nombre de EGEMSA, el software desarrollado (incluido el desarrollado por los contratistas), en el registro intelectual respectivo; bajo la responsabilidad de la Subgerencia de Tecnologías de la Información. Ello a fin de acogerse a los resguardos que estipula la normativa relacionada a la propiedad intelectual[175].

5.8. Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar protección a los activos de información de EGEMSA que son accesibles por los/as contratistas y terceros/as seleccionados/as[176].

EGEMSA, en el marco del cumplimiento de la Seguridad de la Información, establece los siguientes compromisos[177]:

a) Asegurar que la información emitida y/o recibida con los/as terceros/as seleccionados/as y contratistas respete los documentos de gestión interna; mitigando los riesgos asociados con el acceso por parte de los/as terceros/as seleccionados/as y contratistas a los activos de EGEMSA[178].

b) Prever que los/as propietarios/as y custodios de información aseguren que los términos y condiciones para el intercambio de información con los contratistas, que accedan, procesen, almacenen, comuniquen o provean componentes de infraestructura de tecnologías de la información para la información de EGEMSA, se encuentren documentados en un acuerdo[179].

c) Suscribir acuerdos y/o cláusulas de confidencialidad, cuando se requiera información por parte de EGEMSA a los/as terceros/as seleccionados/as y contratistas[180].

d) Supervisar que el monitoreo y la revisión de los servicios externos realizados

por los contratistas cumplan con los términos de seguridad de la información y que los incidentes y problemas en la seguridad de información sean manejados de forma coordinada con la Subgerencia de Tecnologías de la Información[181].

e) Seguimiento y control de las obligaciones en materia de seguridad de la información de los contratistas, lo que se materializará con la emisión de la conformidad, de corresponder[182].

f) Gestionar los cambios a la provisión de servicios por parte de los/as terceros/as seleccionados/as y contratistas, tomando en cuenta aquellos requisitos de seguridad de la información y bajo los lineamientos y/o normativa de cumplimiento por parte de EGEMSA[183].

5.9. Responsabilidades

Las unidades orgánicas, coordinaciones, unidades funcionales de EGEMSA, en el marco de sus funciones establecidas en los documentos de gestión interna y actos resolutivos correspondientes, son responsables de promover el cumplimiento de las Políticas Específicas de Seguridad de la Información de EGEMSA[184].

Es responsabilidad del Oficial de Seguridad y Confianza Digital, la revisión de las presentes políticas específicas de manera anual, o cuando se requiera, ante la existencia de cambios significativos que puedan afectar el Sistema de Gestión de Seguridad de Información en EGEMSA[185].